VIGILANCIA DIGITAL EN MÉXICO

Sursiendo, Comunicación y Cultura Digital, AC.
Chiapas, abril de 2019.

RESUMEN:

Presentamos una recopilación resumida de informaciones e investigaciones relacionadas con la Vigilancia Digital en México, realizada en 2018, con los aportes de organizaciones de derechos digitales e investigadores. Queremos mostrar el panorama de la vigilancia de los últimos años contra activistas, periodistas, académicos y sus familiares, sobre todo en el sexenio de Enrique Peña Nieto, pero que tiene un origen anterior.

Para ello, incluimos algunos **conceptos**, el **marco legal**, las **instancias** responsables y algunos **casos** producidos hasta 2018 (por ejemplo: haciendo mención del *malware* Finfisher, DaVinci y Pegasus), con sus respectivas fuentes referenciadas.

No está incluida la última información, dada a conocer en marzo pasado: **Griselda Triana**, viuda del periodista Javier Valdez, asesinado en Sinaloa en mayo del 2017, denunció ser uno más de los objetivos del ***malware*** **Pegasus**, una herramienta de vigilancia comercializada por la compañía israelí NSO Group, presumiblemente adquirida por el Gobierno de México[1], que sirve como ampliación de la campaña **#GobiernoEspía**, para denunciar estas prácticas opacas y violatorias de derechos humanos.

Esperamos que esta compilación sirva.
Esperamos que paren estas prácticas. Esperamos que se respeten los derechos humanos y se termine la criminalización y represión de la lucha social.

1 "No soy criminal ni terrorista, pero fui espiada": Griselda Triana, viuda de Javier Valdez, fue atacada con Pegasus: https://r3d.mx/2019/03/20/no-soy-criminal-ni-terrorista-pero-fui-espiada-griselda-triana-viuda-de-javier-valdez-fue-atacada-con-pegasus/



INTRODUCCIÓN

Es difícil definir lo que significa el término **vigilancia**. Una primera aproximación puede ser la de David Lyon que lo define como "la atención dirigida, sistemática y cotidiana a detalles personales por motivos de influencia, manejo, protección o dirección"[2].

Pero en la era digital la vigilancia no sólo es cotidiana sino ubicua. La encontramos en todos sitios: es una recolección generalizada de información que ya no necesariamente es dirigida y enfocada. Además, esta vigilancia ya no parece cumplir sólo con los propósitos mencionados sino que va mucho más allá, siendo la estrategia medular de seguridad de muchos estados-nación, además del modelo de negocios de las principales firmas de Internet, compañías de tarjetas de crédito, seguros y publicidad.

La vigilancia a partir de lo digital tomó otro matiz: todo el proceso de transmisión de información puede ser copiado; cada parte del proceso está expuesto a una fácil captura. Entrar en un mundo digital es entrar en un mundo de vigilancia potenciada. También por la naturaleza centralizada de

2 Bauman, Zygmunt y David Lyon (2013) Vigilancia líquida. Paidós.

Internet es posible monitorear casi todo el tráfico mundial desde unas pocas locaciones claves. Ha sido la transición del espionaje ocasional al persistente.

Además de que toda la información es guardada, con varios respaldos por un tiempo ilimitado. La captura, almacenaje y análisis es un proceso automatizado por lo que no requiere grandes esfuerzos, así que deciden capturarlo y guardarlo todo en caso de que alguna vez les fuera útil. La comunicación digital ha hecho que la vigilancia sea muy fácil y que haya una gran dificultad de anonimato.

En resumen, la vigilancia de la comunicación digital es ubicua, automática, efectiva y vive para siempre. Se podrá seguramente encriptar la comunicación pero su patrón de comunicación y las relaciones serán difíciles de proteger de la exposición[3].

Conceptos y puntualizaciones

El ***malware*** es la abreviatura de *malicious software* (software malicioso) término que engloba todo tipo de programa malicioso que funciona para dañar un sistema o causar un mal funcionamiento. Dentro de este grupo podemos encontrar: virus, troyanos, gusanos, *adware, spyware*, entre otros. El ***spyware*** o *software* espía es una aplicación que recopila información sobre una persona u organización sin su conocimiento ni consentimiento. El objetivo más común es distribuirlo a empresas publicitarias u otras organizaciones interesadas[4].

Se dice que la utilización de *malware* es necesario para combatir el espionaje y el crimen organizado. Que es necesario “sacrificar” nuestra privacidad para tener seguridad. Y que el *malware* sólo se usará para quienes estén “atentando” contra “la seguridad nacional”. Sin embargo se ha visto que este no es el caso y que las más de las veces se usa con fines de mercadotecnia y en contra de las periodistas, activistas y defensores de derechos humanos.

Los programas invasivos de vigilancia se usan contra periodistas, opositores políticos y activistas.

3 Sparrow, Elijah (2014) Vigilancia digital https://giswatch.org/es/thematic-report/communications-surveillance/vigilancia-digital

4 Rivero, Marcelo (2016) ¿Qué son los malwares? https://www.infospyware.com/articulos/que-son-los-malwares/

A la fecha, no hemos sabido de un solo caso en el que dichas herramientas hayan ayudado a la captura de algún miembro de los carteles de la droga o relacionado con terrorismo. Y en cambio, los ejemplos contrarios abundan[5].

Los programas utilizados en estos casos se enmarcan en la forma de espionaje llamado de "ataque". El espionaje de la comunicación digital se lleva a cabo bajo dos categorías: ataque y captura.

ATAQUE: Instalación o inoculación de algún software de espionaje que puede hacerse por varias vías: interposición de redes, comprometer físicamente el aparato, *remote exploit* (desde el software por ejemplo), ingeniería social, actualizaciones de software, por medio de terceros, troyanos, errores en los programas.

CAPTURA: La generación de información y metadatos que se hacen en el uso cotidiano de dispositivos de comunicación digital, su envío y almacenaje: aparatos (que en sí mismo ya tienen protocolos de captura de información), emisiones de los aparatos, redes, terceros (provedores de Internet, compañías de tarjetas, etc).

Para que puedan instalarse estos programas considerados de ataque, o softwares de espionaje se llevan a cabo distintas técnicas. Una de las formas más común para instalar este tipo de software es por medio de la **ingeniería social**.

La ingeniería social es la práctica de obtener información confidencial a través de la manipulación de usuarios. A través de conocer con quiénes interactúa, de qué manera interactúa y sus prácticas de comunicación y navegación habituales se engaña a la persona para abrir un enlace que infecta su aparato o que de información confidencial. El principio que sustenta la ingeniería social es el que en cualquier sistema "los usuarios son el eslabón débil". En la práctica, un ingeniero social usará comúnmente el teléfono o Internet para engañar a la gente, fingiendo ser, por ejemplo, un empleado de algún banco o alguna otra empresa, un compañero de trabajo, un

5 Pérez de Acha, Gisela (2017) ¿Quién está utilizando malware en México? https://www.derechosdigitales.org/10874/quien-esta-utilizando-malware-en-mexico/

técnico o un cliente[6]. La ingeniería social se define como un método basado en el engaño y la persuasión que puede llevarse a cabo a través de canales tecnológicos o bien en persona, y que se utiliza para obtener información significativa o lograr que la víctima realice un determinado acto[7]. Además de la ingeniería social también hay programas que generalmente se aprovechan de las fallas mismas en los sistemas o tecnologías para poder instalarse. El uso de "**exploits**" es común en casi todos los métodos. Estos se aprovechan de los errores (bugs) y vulnerabilidades en sistemas computacionales con el propósito de introducir programas o funciones no consentidas por el usuario. En esta categoría, la empresa Hacking Team ofrece la posibilidad de usar un tipo de exploit bastante controversial: los códigos maliciosos secretos o no revelados (zero-day) que aprovechan fallos de software no conocidos públicamente y que, por ende, no han sido comunicados a su desarrollador ni consecuentemente reparados. De ahí que se les llame "de día cero", en función de que no ha existido tiempo de reacción entre el descubrimiento de la vulnerabilidad y la adopción de alguna medida que se haga cargo de ella[8].

A veces la información que se guarda o que se recoge es algo más que el contenido mismo, la información o los datos que se generan a partir de esa información. A esto se le llama **metadatos** cuya definición sencilla es simplemente "los datos sobre los datos".

Se podría ejemplificar con las fichas de una biblioteca (metadatos) y los libros (datos). Mientras que las fichas tienen toda la información relacionada con el autor, el título, el ISBN, el año, la editorial, en el libro está el contenido que normalmente un usuario buscará.

En el mundo digital sucede con otros elementos, por ejemplo las fotografías digitales. Cuando se toma una fotografía lo que pocas veces nos enteramos es que mientras la cámara captura las imágenes, va guardando en forma de metadatos, información de cómo fue tomada la fotografía: fecha, hora, diafragma, velocidad, uso de flash, modo de captura, entre otros datos, geoposicionamiento satelital en algunos casos.

Los metadatos de comunicaciones son datos sobre las comunicaciones de una persona, por

6 Wikipedia: Ingeniería social (seguridad informática) https://es.wikipedia.org/wiki/Ingenier%C3%ADa_social_(seguridad_inform%C3%A1tica)

7 "Ingeniería social" (s/f) Departamento de Seguridad Informática de la Universidad Nacional de Luján. http://www.seguridadinformatica.unlu.edu.ar/?q=taxonomy/term/11

8 Pérez de Acha, Gisela (2016) Informe: Hacking Team: Malware para la vigilancia en América Latina https://www.derechosdigitales.org/wp-content/uploads/malware-para-la-vigilancia.pdf

ejemplo: los números telefónicos de origen y destino de una comunicación; la hora, fecha y duración de la misma; los datos de identificación de la tarjeta SIM (IMSI) y del dispositivo (IMEI); e incluso los datos de localización de las antenas a las cuáles se conecta un dispositivo móvil[9].

De manera frecuente se pretende minimizar cuán invasiva puede ser la recolección, almacenamiento y análisis de metadatos de comunicaciones, en particular respecto del contenido de las comunicaciones.

Sin embargo, **los metadatos de comunicaciones pueden revelar tanta o mucha más información personal que el contenido mismo de las comunicaciones[10].**

En México ha habido varios casos de compra de software espía y uso de éste contra activistas, periodistas, defensoxs de los derechos humanos. Por lo que es importante conocer esta información y el marco legal en el que se desarrolla.

MARCO LEGAL

El derecho a la privacidad está protegido por la Constitución Política de los Estados Unidos Mexicanos. Ahí se establece que la información que se refiere a la vida privada (de su persona, familia, residencia, documentos o posesiones) será protegida. También, la Constitución reconoce el respeto a los derechos humanos, así como a los compromisos que México ha firmado en tratados internacionales. Sin embargo, fue hasta el año **2007** que México comenzó a legislar en el ámbito de la protección de datos: se modificó la Constitución con objeto de garantizar el derecho a la protección de datos y se estableció que cualquier interferencia en las comunicaciones debe ser aprobada por un juez federal, es el único que puede autorizar la vigilancia de comunicaciones privadas y sólo cuando los funcionarios demuestran que tienen un caso bien armado para realizar esa solicitud. En el artículo 16 constitucional se estipula la garantía de inviolabilidad de comunicaciones[11].

9 Red en Defensa de los Derechos Digitales (R3D) (2016) El estado de la Vigilancia: Fuera de control. https://r3d.mx/wp-content/uploads/R3D-edovigilancia2016.pdf

10 Red en Defensa de los Derechos Digitales (R3D) (2016) El estado de la Vigilancia: Fuera de control. https://r3d.mx/wp-content/uploads/R3D-edovigilancia2016.pdf

11 SonTusDatos (2014) El caso FinFisher https://www.giswatch.org/hu/node/4955

En julio de 2010, el Congreso de la Unión promulgó la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP). Su ámbito de aplicación incluye a los individuos y las empresas, no a los gobiernos ni a otras entidades públicas[12]. Es la única ley federal que rige la privacidad y protección de datos en posesión de particulares.
El Instituto Federal de Acceso a la Información y Protección de Datos (IFAI) es la institución autónoma encargada de salvaguardar los derechos individuales a la protección de datos. En principio, el IFAI sólo existía para garantizar el derecho de los ciudadanos a acceder a la información pública gubernamental. Sin embargo, desde 2010 sus atribuciones se ampliaron con objeto de garantizar también el derecho a la protección de datos personales[13].

Tanto la Corte Suprema y la Corte Interamericana de los Derechos Humanos, cuya ley es vinculante para todas las autoridades judiciales en México, han reconocido que el derecho a la inviolabilidad de las comunicaciones privadas protege no sólo el contenido de las comunicaciones sino también los datos que identifican dicha comunicación, o "tráfico de datos de comunicación", tales como la identidad de las personas en comunicación, la duración de la comunicación, la localzación geográfica, y la identificación del IP (protocolo de acceso a Internet).

La Suprema Corte también ha dictaminado que las comunicaciones privadas están protegidas constitucionalmente de vigilancia en tiempo real, así como de interferencia subsecuente en el hardware donde la comunicación se almacena.

En este sentido, la Constitución garantiza el derecho del individuo a la privacidad y protección de datos, salvo algunas excepciones, como en el caso de una invasión militar, alteración grave de la paz, o de cualquier otro evento que ponga a la sociedad en peligro o conflicto grave. De acuerdo con la Constitución, sólo la autoridad judicial federal puede autorizar escuchas telefónicas y la interceptación de comunicaciones privadas, a petición de la autoridad federal competente o la Procuraduría General de la República[14].

12 SonTusDatos (2014) El caso FinFisher
https://www.giswatch.org/hu/node/4955
13 SonTusDatos (2014) El caso FinFisher
https://www.giswatch.org/hu/node/4955
14 SonTusDatos (2014) El caso FinFisher
https://www.giswatch.org/hu/node/4955

De acuerdo con el Código Nacional de Procedimientos Penales y otras leyes generales, solamente las agencias del Ministerio público y Fiscalías, además de órganos de inteligencia, están facultados para realizar una intromisión de comunicaciones privadas y siempre dentro del marco de una averiguación previa[15] .

La prohibición del espionaje es explícita en la Constitución, y también existe un marco jurídico para protección de datos personales respecto a particulares, pero en cuanto el espionaje es gubernamental, el marco legal es laxo[16] . Además el IFAI es responsable de garantizar el derecho del titular a la protección de sus datos personales. En este caso, sin embargo, su papel no está claro: puede investigar, como ya lo ha hecho, y emitir multas. Pero no hay ningún procedimiento establecido para casos de vigilancia gubernamental. También, como la cuestión en juego es una violación de derechos humanos, otra institución que podría jugar un papel relevante es la Comisión Nacional de Derechos Humanos (CNDH). Sin embargo, esa institución sólo puede hacer recomendaciones que no son vinculantes[17] .

¿Quiénes sí nos pueden espiar?

La excepción para la intervención de comunicaciones se establece con el control del Poder Judicial, que se supone debe autorizarla. Sin embargo, advierte que ese tipo de actividades las realizan los gobiernos de manera oculta y al margen de la ley[18] .

En México, no existe regulación específica de herramientas altamente intrusivas de vigilancia como el uso de software espía. No obstante, la legislación reconoce la posibilidad de que algunas autoridades puedan requerir autorización judicial federal para la intervención de comunicaciones privadas para fines específicos[19] .

15 Angel, Arturo (2015) México, el principal cliente de una empresa que vende software para espiar. Animal Político. https://www.animalpolitico.com/2015/07/empresa-de-hackers-exhibida-por-venta-de-software-espia-a-paises-represores-y-mexico-resulta-su-principal-cliente/

16 Rodríguez García, Arturo (2017) El caso Maloof y el software malicioso FinFisher. Revista Proceso. https://www.proceso.com.mx/491735/caso-maloof-software-malicioso-finfisher

17 SonTusDatos (2014) El caso FinFisher. https://www.giswatch.org/hu/node/4955

18 Rodríguez García, Arturo (2017) El caso Maloof y el software malicioso FinFisher. Revista Proceso. https://www.proceso.com.mx/491735/caso-maloof-software-malicioso-finfisher

19 Red en Defensa de los Derechos Digitales (R3D) (2017) Gobierno Espía. Vigilancia sistemática a periodistas y defensores de derechos humanos en México.

A nivel federal existen varias autoridades que tiene el poder de solicitar vigilancia de las comunicaciones privadas.

1. Procuraduría General de la República y Procuradurías de las entidades federativas tiene ese poder de acuerdo al Código Nacional de Procedimientos Penales que fue modificado en el 2009 con ese propósito. Contempla la intervención de comunicaciones privadas en casos en los que le Ministerio Público lo considere necesario para la investigación de algún delito. Los artículos 292 a 302 detallan el procedimiento a seguir, incluyendo los requisitos y plazos de la solicitud de autorización judicial. Además la Ley General para Prevenir y Sancionar los Delitos en Materia de Secuestro del 2010 y la Ley contra la Delincuencia Organizada del 2007 dan a la PGR la facultad de espiar en conversaciones privadas, regulando esta intervención de manera similar al Código Nacional de Procedimientos Penales.

2. Policía Federal : La Ley de la Policía Federal aprobada en el 2009 autoriza a la policía interceptar las comunicaciones privadas para prevenir algunas ofensas criminales. Establece, en su artículo 48, que la intervención de comunicaciones privadas únicamente puede autorizarse cuando "se constate la existencia de indicios suficientes que acrediten que se está organizando" la comisión de una ciertos delitos definidos en la ley. El procedimiento de solicitud de autorización se regula de manera específica en los artículos 48 a 55.

3. Centro de Investigación y Seguridad Nacional (CISEN): La Ley de Seguridad Nacional establece, en el artículo 33 y siguientes, que la intervención de comunicaciones privadas únicamente puede solicitarse en casos de "amenaza inminente a la seguridad nacional" detallados en el artículo 5 de la ley, previa autorización judicial federal[20]. (*Actualización: en el nuevo Gobierno se suprime este Centro*)

En otros temas de vigilancia el Sistema Nacional de Seguridad Pública autoriza a todos los agentes de la policía a conducir actividades de recolección de información por medio de "sistemas estandarizados". Finalmente, el estado federal y hasta las leyes municipales contienen disposiciones para bloquear, restringir o vigilar las comunicaciones en centros de detención.

https://r3d.mx/2017/06/19/gobierno-espia/

20 Red en Defensa de los Derechos Digitales (R3D) (2017) Gobierno Espía. Vigilancia sistemática a periodistas y defensores de derechos humanos en México.
https://r3d.mx/2017/06/19/gobierno-espia/

Las leyes arriba mencionadas incluyen las comunicaciones de Internet entre aquellas comunicaciones sujetas a ser interceptadas conforme a una orden judicial de un juez federal. Aquellas leyes no establecen ninguna garantía contra el abuso, como la supervisión de una instancia independiente, requerimientos de transparencia, o aviso subsecuente a la persona afectada por las medidas de vigilancia.

NUEVAS LEYES/MODIFICACIONES EN LEYES DE COMUNICACIÓN Y VIGILANCIA

2009, Ley Federal de Telecomunicaciones. Fue modificada para que los provedores de servicios de telecomunicaciones guardaran el tráfico de datos de comunicación (**metadatos**) incluyendo el tipo de comunicación, los servicios utilizados, el origen y el destino de las comunicaciones, fecha, hora y duración de las comunicaciones y hasta la localización geográfica de los dispositivos de comunicación. Tienen la obligación de guardar estos datos por al menos doce meses, y aplica para todos los usuarios de servicios brindados por parte de las empresas de telecomunicaciones. Además permite a la Fiscalía General de la República y la Fiscalía Estatal acceder a estos datos para la investigación de ofensas criminales serias sin la necesidad de una orden judicial[21].

2012 Ley Federal de Telecomunicaciones. Fue nuevamente modificada estableciendo que las empresas de telecomunicaciones tienen la obligación de cooperar con la Fiscalía General y la Fiscalía Estatal para proveer la localización geográfica en tiempo real de dispositivos celulares de comunicación sin la necesidad de una orden judicial.

2013 fue un año de enmiendas que buscaron criminalizar o detener la protesta social y limitar la libertad de expresión y libre asociación. Como el cambio al artículo 362 de código penal de la Ciudad de México y al Código Penal Nacional en el Congreso Federal, las leyes sobre demostraciones públicas en Jalisco, San Luis Potosí y la Ciudad de México, así como aquellas decretadas en Quintana Roo y Chiapas.

2014 Reforma de telecomunicaciones. Incluye la ampliación de métodos de vigilancia en las

21 Red en Defensa de los Derechos Digitales (R3D) (2016) Vigilancia Estatal de las Comunicaciones y Protección de los Derechos Fundamentales en México.

comunicaciones. Se incrementa la retención de datos a un periodo de 24 meses y permite que los datos sean almacenados por tiempo indefinido con la sola solicitud de una autoridad de gobierno. También permite que autoridades fuera del sistema penal, como el CISEN, el ejército, la armada, y la policía federal, puedan determinar la localización geográfica de los dispositivos de comunicación móvil en tiempo real y acceder a los datos guardados por las compañías de telecomunicaciones sin tener que asegurar una orden judicial, bajo la vaga y ambigua premisa del "ejercicio de poderes inherente a la producción de inteligencia".

2016 El Código Nacional de Procedimientos Penales, que reemplaza al Código Federal de Procedimientos Penales y los 32 Códigos Estatales, fue impulsado desde el 2014. Este nuevo Código que es implementado por etapas y está en pleno ejercicio desde junio del 2016 reitera los poderes de vigilancia de las autoridades fiscales. Un avance importante es que el Código sí requiere de la autorización judicial para la intercepción de todo tipo de comunicaciones, incluyendo los metadatos, ya sea en tiempo real o para su retención.

Sin embargo, la posibilidad de monitorear la geolocalización en tiempo real de los dispositivos moviles continúa en este nuevo Código, también permite la retención de datos de redes, sistemas y computadoras sean confiscadas o utilizadas sin una orden judicial. El Código también falla en agregar garantías adecuadas como la supervisión externa, medidas de transparencia o mecanismos para dar aviso diferido a los usuarios afectados.

En los últimos cinco años las leyes, las regulaciones de vigilancia, y el presupuesto nacional en México han sufrido cambios drásticos. Sobre el trasfondo de la mal llamada "guerra contra el narco", e impulsado por acuerdos de cooperación internacional sobre seguridad como la "Iniciativa Mérida", México ha experimentado una serie de reformas legales que permiten un incremento en los poderes y técnicas de vigilancia disponibles para las agencias de seguridad, ya sea para la investigación y procesamiento de crímenes o para la prevención de amenazas a la seguridad nacional.

El 99% de la utilización de actos de vigilancia a las comunicaciones se hacen de manera ilegal. La laxitud del Estado mexicano frente a la práctica de espionaje para darle un uso político no ha

variado ni siquiera con los numerosos casos registrados al convertirse en escándalo a partir de filtraciones a la prensa en diferentes coyunturas.

Está claro que las técnicas y poderes de espionaje no son utilizados para prevenir “amenazas a la seguridad nacional” o para detener crímenes, o al narcotráfico. La más de las veces son utilizados contra aquellas personas que retan o cuestionan las prácticas del poder actual, defensores de derechos humanos, periodistas, activistas, etc. En los últimos años se ha destapado una serie de programas utilizados por el gobierno de México para espiar a dichos actores, ya que una parte medular de la estrategia ha sido mantener mano de hierro sobre los medios de comunicación y silenciar las voces críticas, incluyendo aquellas de la Internet, así limitar la libertad de expresión. En esta coyuntura los gobiernos donde hay menor supervisión ciudadana, legislativa y judicial han reforzado su control sobre la opinión pública por medio de todo tipo de métodos, desde la compra de publicidad hasta amenazas y ataques físicos a personas que se dedican a la comunicación.

CASOS DE VIGILANCIA

2010: Chiapas. Arresto de Héctor Bautista miembro de la comunidad de software libre y administrador de la página InfoChiapas.com fue arrestado por la policía estatal por cargos de pornografía infantil. Fue confiscada su computadora y sus tarjetas de memoria. Realmente fue arrestado por la publicación de un artículo que hablaba de la deuda del gobierno. Estuvo 40 días en custodia y después fue liberado.

2011: Veracruz. Maruchi Bravo y Gilberto Martínez fueron acusados de terrorismo y sabotaje, como autores de las amenazas a los ataques de las escuelas en Veracruz. Simplemente el gobierno quería criminalizar a estas personas que utilizaban las redes sociales para transmitir información importante para la ciudadanía.

2013 #OP5 Puebla. Iván Guizasola Vázquez, Néstor López Espinosa y Eduardo Salazar Velázquez fueron arrestados tras convocar a una marcha para el 5 de mayo por medio de Facebook. Tal protesta se canceló por la intervención policial donde se registró la casa de quienes participarían, llevando interrogatorios con métodos de tortura. Las tres personas estuvieron una semana en custodia.

2013. Chiapas. Gustavo Maldonado. Acusado de narcomenudeo y arrestado el 8 de agosto del 2013 bajo un caso lleno de irregularidades. Gustavo es crítico con el gobierno de Chiapas en redes sociales digitales, y en meses pasados había llamado a manifestaciones por el tema del agua en Tuxtla. La tarde de su arresto había publicado un video y retuiteado información sobre la compra de Blackeyed Hosting Monitos, equipo de vigilancia para localizar activistas digitales en Chiapas. Maldonado fue liberado después de haber estado 90 días detenido.

2013. Lydia Cacho. En septiembre la periodista pulicó un artículo titulado "Ciberterrorismo de Estado" donde denunció varios casos de hostigamiento por organizaciones supuestamente vinculadas a partidos políticos en el poder. El artículo da cuenta de las acciones llevadas a cabo contra periodistas y de las técnicas de falsificación de opinion en medios sociales para generar una opinión favorable del gobierno. Empezó, además a ser acosada y hostigada.

2013 censura de la página **1dmx.org**. Página web que servía como plataforma para la difusión de evidencia de violaciones a los derechos humanos que ocurrieron durante las protestas a la toma de poder de Enrique Peña Nieto. El 2 de diciembre la empresa estadounidence GoDaddy.com informó a la administración de 1dmx.org de la suspensión de su dominio. Les comunicaban que dicha suspensión era parte de una investigación policial y si querían mayor información debían contactarse con un oficial de seguridad nacional de la embajada de Estados Unidos en México. Se les informó además qe la agencia responsible por la solicitud fue el Centro Especializado en Respuesta Tecnología (CERT), una división de Comisión Nacional de Seguridad (CNS – Policía Federal) bajo el Ministerio Federal de Asuntos Interiores.

El 4 de marzo del 2015, 1dmx.org hizo público el caso, en menos de 24 horas el dominio fue restaurado sin ninguna explicación.

Adquisición y uso de equipo de vigilancia por el gobierno mexicano (2007 – 2014)

Desde el 2007 han habido reportes sobre la cooperación del gobierno mexicano con el de Estados Unidos para intervenir llamadas telefónicas y correos electrónicos con el equipo de la compañia Verint dada al gobierno mexicano, que tiene la capacidad de interceptar hasta 3 millones de comunicaciones. Es una operación del gobierno mexicano financiado por los Estados Unidos.

En **2012** se hizo público que el Departamento de Defensa Nacional tenía contratos para adquirir tecnología de vigilancia y equipo con capacidad para monitorear correos, interferencia de voz, ruido de fondo, captura de imágenes, extracción de sms y mms, listas de contactos, registros de calendarios, localización gps y capturas de pantallas, acceso y manipulación de los documentos del sistema, información de la tarjeta SIM, información de hardware, etc.

En **2013** se publicó la existencia del software de cibervigilancia **Finfisher** en varios países incluyendo México.

En **2013,** Impacto publicó parte de los contratos de la Oficina de la Procuraduría General para comprar equipo y licencias de uso para el software de vigilancia "Plint Tracking Locsys" y "Hunter". El propósito de estos contratos es tener la tecnología para localizar aparatos de comunicación en tiempo real.

2013 Citizen Lab reportó sobre el uso del software de vigilancia "DaVinci" diseñado por **Hacking Team** en varios países, incluyendo México, y apuntó que se había estado usando en otros países en contra de activistas y periodistas.

CASOS CONCRETOS DE UTILIZACIÓN DE SOFTWARE DE ESPIONAJE EN MÉXICO

FinFisher

FinFisher es un software de espionaje de la empresa **Gamma Group** de origen angloalemán. Es un malware que se hace pasar por otro software, entra en computadoras y celulares y toma control total del dispositivo. Infecta los aparatos más que por ingeniería social, por imitación de enlaces falsos que parecen reales, tipo iTunes, Mozilla etc. Este software para instalarse requiere que la víctima descargue enlaces de actualizaciones de software falsas de fuentes aparentemente confiables como Adobe Flash, iTunes, BlackBerry, entre otros. Una vez instalado en un sistema de cómputo, un tercero puede controlar y acceder a la información cada vez que el dispositivo esté conectado al Internet.

Se supone que se vende únicamente a oficiales de seguridad nacional, **Gamma International** dice que sólo vende a gobiernos.

En **marzo** del **2013** Citizen Lab sacó un reporte de utilización de FinFisher en México operando en dos redes de telecomunicaciones Iusacell y UniNet. Detectó que en 25 países se aloja el programa en sus servidores. Informes previos han revelado que activistas y miembros de la oposición política en todo el mundo han sido intervenidos tanto en sus teléfonos como en sus computadoras a través de FinFisher[22].

Las empresas implicadas en el caso mexicano (Uninet y Iusacell) respondieron en agosto de 2013 que no tenían equipos con FinFisher instalado dentro de sus centros de datos, pero como señaló el activista Jacobo Nájera, tampoco descartaron la posibilidad de que alguno de sus usuarios lo estuviera haciendo. Así mismo, el Citizen Lab reportó que, al menos hasta septiembre de 2013, se tenía información de que el programa seguía activo dentro de las redes monitoreadas[23].

El **20 de junio de 2013**, las asociaciones civiles mexicanas, ContingenteMX, Propuesta Cívica y Al Consumidor, presentaron una denuncia ante el IFAI lo cual dio lugar a que la autoridad pudiera investigar tanto a Iusacell como Uninet con el objetivo de conocer el uso de FinFisher en sus servidores[24].

Julio de 2013: Investigación periodística del diario *Reforma* halló que la empresa Obses de México vendió FinFisher a la Procuraduría General de la República, así como a otras instancias de seguridad en el país[25].

La Procuraduría Geneneral de la República había pagado casi 109 millones pesos (aproximadamente 8 millones de dólares) por el software FinFisher y alrededor de 93 millones de pesos (alrededor de 7 millones de dólares) para un sistema de seguimiento por satélite llamado

22 SonTusDatos (2014) El caso FinFisher. https://www.giswatch.org/hu/node/4955
23 Flores, Pepe (2015) FinFisher en México: Sonríe, te siguen espiando. https://www.digitalrightslac.net/es/finfisher-en-mexico-sonrie-te-siguen-espiando/
24 SonTusDatos (2014) El caso FinFisher. https://www.giswatch.org/hu/node/4955
25 Flores, Pepe (2015) FinFisher en México: Sonríe, te siguen espiando. https://www.digitalrightslac.net/es/finfisher-en-mexico-sonrie-te-siguen-espiando/

Hunter Punt Tracking / Locsys. Ambas compras fueron hechas por la empresa mexicana Obses, el contrato era demasiado costoso, por lo que IFAI investiga, Obses se protege con “convenios de confidencialidad” y se le multa de un millón 300 mil pesos[26].

11 de julio de 2013, los activistas de derechos humanos del grupo Desobediencia Civil informaron que habían encontrado rastros del programa FinFisher en sus teléfonos celulares y sus computadoras y que habían recibido varias amenazas indefinidas[27].

Septiembre de 2014: filtración de WikiLeaks que demostró que Gamma International sí está al tanto de quiénes distribuyen su software y con qué propósitos; además de notificar sobre la visita de los dueños de esta empresa en instalaciones gubernamentales de México en 2013[28].

4 de agosto de 2014, un hacker con el apodo de **PhineasFisher** anunció que había hackeado FinFisher y publicó diversos documentos confidenciales en Internet. Entre éstos se encontraban lo que parecen ser registros auténticos de clientes, manuales, folletos, listas de precios y el código fuente. De acuerdo con una descripción de la información filtrada, es interesante observar que, en la lista de clientes, aparece el nombre de usuario "Cobham", probablemente refiriéndose al Grupo de Cobham, cuya división "Cobham Defence Electronics" construye productos para aplicaciones de defensa, médicos, industriales y comerciales en México[29].

Una investigación independiente conducida por ContingenteMX y Propuesta Cívica halló que FinFisher había sido empleado por al menos cuatro dependencias de seguridad en México: la Secretaría de Seguridad Pública, la Procuraduría General de la República, el Centro de Investigación y Seguridad Nacional, y el Estado Mayor Presidencial[30].

El reporte de García y Robles sitúa a México entre los cinco principales compradores de

26 SonTusDatos (2014) El caso FinFisher. https://www.giswatch.org/hu/node/4955
27 SonTusDatos (2014) El caso FinFisher. https://www.giswatch.org/hu/node/4955
28 SonTusDatos (2014) El caso FinFisher. https://www.giswatch.org/hu/node/4955
29 SonTusDatos (2014) El caso FinFisher. https://www.giswatch.org/hu/node/4955
30 Flores, Pepe (2015) FinFisher en México: Sonríe, te siguen espiando. https://www.digitalrightslac.net/es/finfisher-en-mexico-sonrie-te-siguen-espiando/

tecnología de vigilancia. Indicios de que esta tecnología está siendo empleada al menos en Chiapas, Coahuila, Quintana Roo, Puebla, Tamaulipas y Veracruz[31].

Un informe del Monitor Mundial sobre la Sociedad de la Información (MMSI), entregado a la Cámara de Diputados el 14 de abril de 2015, advirtió la debilidad del derecho mexicano para proteger a los ciudadanos frente a las tareas de espionaje gubernamental, con base al caso FinFisher:

"El espionaje gubernamental es un tema delicado porque no siempre está claro si las autoridades están actuando para proteger los intereses de seguridad nacional o si van más allá de sus obligaciones y comienzan a infringir los derechos humanos de los ciudadanos".

"Es precisamente debido a que no siempre son claros los límites y a que las instituciones son falibles, que deberían existir reglas y procedimientos específicos para salvaguardar los derechos humanos, así como las normas de rendición de cuentas y supervisión que el gobierno debe cumplir"[32].

Hay indicios suficientes de que las medidas de vigilancia son usadas contra defensores de derechos humanos, activistas y periodistas[33].

Pegasus

Pegasus es un spyware de intercepción legal para gobiernos fabricada por **NSO Group**, empresa de origen israelí. Inocula generalmente por ingeniería social mandando mensajes con links que infectan los dispositivos. Para obtener el clic que permite la infección del dispositivo, el atacante debe asegurarse de engañar al objetivo. Para ello, se envían mensajes diseñados para aparentar ser legítimos. En este punto, cobra especial relevancia la infraestructura de NSO Group, ya que los dominios que pertenecen a esta buscan suplantar a otros sitios legítimos como medios de comunicación, servicios de telecomunicaciones, redes sociales, portales de gobierno, organizaciones

31 Flores, Pepe (2015) FinFisher en México: Sonríe, te siguen espiando. https://www.digitalrightslac.net/es/finfisher-en-mexico-sonrie-te-siguen-espiando/

32 Rodríguez García, Arturo (2017) El caso Maloof y el software malicioso FinFisher. Revista Proceso. https://www.proceso.com.mx/491735/caso-maloof-software-malicioso-finfisher

33 Flores, Pepe (2015) FinFisher en México: Sonríe, te siguen espiando. https://www.digitalrightslac.net/es/finfisher-en-mexico-sonrie-te-siguen-espiando/

humanitarias, aerolíneas, entre otros[34].

Los investigadores del Citizen Lab hallaron que, dentro de los dominios identificados dentro de la infraestructura de NSO Group, **la mayoría refieren a México** y los Emiratos Árabes Unidos. Entre los dominios con algún vínculo a sitios web en México se encontraron, entre otros[35]:

Unonoticias.net, Univision.click, Iusacell-movil.com.mx, Y0utube.com.mx, Fb-accounts.com, Googleplay-store.com, Whatsapp-app.com

Una vez que el objetivo hace clic en el enlace, el sitio web empleado para la infección (denominado *Anonymizer*) envía una solicitud al servidor de instalación del spyware (Pegasus Installation Server) ubicado en las instalaciones de quien opera el ataque. Este servidor examina si el dispositivo a infectar tiene una vulnerabilidad que el spyware pueda explotar, como la del Trident en iOS (El Citizen Lab descubrió que Pegasus explotaba una vulnerabilidad de seguridad inédita (*zero-day exploit*) en el sistema operativo iOS, bautizada como Trident). Existen dos escenarios posibles:

- Si el dispositivo posee una vulnerabilidad, el servidor envía el exploit adecuado a través del sitio web (*Anonymizer*) para intentar una infección.
- Si la infección falla por cualquier motivo, el navegador del objetivo será redirigido a un sitio web legítimo determinado previamente por el atacante, con la finalidad de evitar suspicacias.

Además de obtener los permisos previamente descritos, el spyware envía la información recolectada al *Pegasus Data Server* a través de la P*egasus Anonymizing Transmission Network*, un sistema de proxies en cadena. Eso permite que el atacante pueda visualizar y procesar la información obtenida en una estación de trabajo (*Pegasus Working Station)*[36].

Otra característica encontrada del spyware es que, una vez que infecta el dispositivo, deshabilita

34 Red en Defensa de los Derechos Digitales (R3D) (2016) El estado de la Vigilancia: Fuera de control. https://r3d.mx/wp-content/uploads/R3D-edovigilancia2016.pdf

35 Red en Defensa de los Derechos Digitales (R3D) (2017) Destapa la vigilancia: promotores del impuesto al refresco, espiados con malware gubernamental. https://r3d.mx/2017/02/11/destapa-la-vigilancia-promotores-del-impuesto-al-refresco-espiados-con-malware-gubernamental/

36 Red en Defensa de los Derechos Digitales (R3D) (2016) El estado de la Vigilancia: Fuera de control. https://r3d.mx/wp-content/uploads/R3D-edovigilancia2016.pdf

las actualizaciones automáticas del sistema operativo para garantizar su persistencia; también detecta y remueve otros jailbreaks en el aparato.

El software conocido como Pegasus se infiltra en los teléfonos inteligentes y otros aparatos para monitorear cualquier detalle de la vida diaria de una persona por medio de su celular: llamadas, mensajes de texto, correos electrónicos, contactos y calendarios. Incluso puede utilizar el micrófono y la cámara de los teléfonos para realizar vigilancia; el teléfono de la persona vigilada se convierte en un micrófono oculto[37]. La instalación de este sofisticado spyware permite al atacante tomar control de diferentes funciones y acceder a los contenidos del aparato. Entre los permisos adquiridos, se encuentran:

- Acceso a la información guardada en el dispositivo como: archivos, datos del calendario, listas de contactos, contraseñas, entre otros.
- Acceso a mensajes de texto, así como datos de otras aplicaciones como Gmail, WhatsApp, Skype, Facebook, Telegram.
- Acceso a escuchar llamadas realizadas por teléfono, a través de WhatsApp o Viber.
- Permisos para grabar activa o pasivamente utilizando el micrófono y la cámara del dispositivo[38].

Desde 2011, al menos tres agencias federales mexicanas han gastado casi 80 millones de dólares en programas de espionaje de una empresa de origen israelí (NSO Group).

La empresa afirma que vende la herramienta de forma exclusiva a los gobiernos con la condición de que solo sea utilizada para combatir a terroristas o grupos criminales y carteles de drogas como los que han violentado a los mexicanos desde hace mucho tiempo.

Sin embargo, según decenas de mensajes examinados por The New York Times y analistas forenses independientes, el software ha sido utilizado para vigilar a algunas de las personas que

37 Ahmed, Azam y Nicole Perlroth (2017) 'Somos los nuevos enemigos del Estado': el espionaje a activistas y periodistas en México. New York Times.
https://www.nytimes.com/es/2017/06/19/mexico-pegasus-nso-group-espionaje/

38 Red en Defensa de los Derechos Digitales (2017) Promotores del impuesto al refresco, espiados con malware gubernamental. Lado B.
https://ladobe.com.mx/2017/02/destapa-la-vigilancia-promotores-del-impuesto-al-refresco-espiados-malware-gubernamental/

han sido más críticas del gobierno, así como a sus familiares, lo que muchos ven como un intento sin precedentes para debilitar e intimidar a la gente que intenta ponerle fin a la corrupción que afecta a la sociedad mexicana[39].

CASOS DE PEGASUS EN MÉXICO

2012: Estado mexicano pagó 20 millones a NSO Group.
2015: uno de los responsables de la investigación periodística de la Casa Blanca de Enrique Peña Nieto, **Rafael Cabrera**, recibió varios mensajes asociados con la infraestructura de NSO Gruoup en agosto de 2015.

Como ha señalado previamente R3D en su informe El Estado de la Vigilancia, existen varios indicios de la adquisición de equipo de NSO Group para parte de distintas instancias del gobierno de México, tales como la Secretaría de la Defensa Nacional, la Procuraduría General de la República y el Centro de Investigación y Seguridad Nacional[40]. Hay pues evidencia documentada de la adquisisción de Pegasus por pate de dependencias del gobierno federal.

Se enlistan los casos concretos donde se documentó el ataque con Pegasus a periodistas, activistas, defensorxs de derechos humanos, que son dos más que los 19 casos documentados por Citizen Lab:

Espionaje a periodistas

- 1. Carmen Aristegui
- 2. Emilio Aristegui, hijo de Carmen Aristegui (menor, no es periodista)
- 3. Rafael Cabrera
- 4. Sebastián Barragán
- 5. Carlos Loret de Mola
- 6. Daniel Lizárraga

39 Ahmed, Azam y Nicole Perlroth (2017) 'Somos los nuevos enemigos del Estado': el espionaje a activistas y periodistas en México. New York Times.
https://www.nytimes.com/es/2017/06/19/mexico-pegasus-nso-group-espionaje/
40 Red en Defensa de los Derechos Digitales (R3D) (2017) Destapa la vigilancia: promotores del impuesto al refresco, espiados con malware gubernamental.
https://r3d.mx/2017/02/11/destapa-la-vigilancia-promotores-del-impuesto-al-refresco-espiados-con-malware-gubernamental/

- 7. Salvador Camarena

Miembros del Centro Miguel Agustín Pro Juárez

- 8. Mario Patrón
- 9. Stephanie Brewer
- 10. Santiago Aguirre

Promotores del impuesto a refrescos

- 11. Alejandro Calvillo
- 12. Luis Encarnación
- 13. Simón Barquera

Políticos

- 14. Roberto Gil Zuarth
- 15. Ricardo Anaya
- 16. Fernando Rodríguez Doval

Instituto Mexicano para la Competitividad

- 17. Juan Pardinas
- 18. Alexandra Zapata

Investigadores internacionales

- 19. Miembros del GIEI que investigaban la desaparición de los 43 estudiantes de Ayotzinapa

Los dos abogados del "caso Narvarte"

- 20. Karla Micheel Salas
- 21. David Peña

De los 88 mensajes de texto con enlaces maliciosos que han sido documentados, el dominio con mayor uso fue smsmensaje[.]mx, con 44.3% de los enlaces (39), seguido de unonoticias[.]net, con 31.8 por ciento (28)[41].

Sobre los periodos con más intentos de infección, la mayoría de los mensajes se mandó en mayo de 2016 (22), julio de 2016 (16), agosto de 2015 (11) y junio de 2016 (10). Si se desglosa por años, en 2015 se realizaron 25 intentos de infección documentados (28.4 por ciento), mientras que en

41 Red en Defensa de los Derechos Digitales (R3D) (2017) Gobierno Espía. Vigilancia sistemática a periodistas y defensores de derechos humanos en México.
https://r3d.mx/2017/06/19/gobierno-espia/

2016 se mandaron 63 mensajes (71.6 por ciento)[42].

Se ve que durante coyunturas críticas es cuando más mensajes o intento de infección se mandan. Al contrastar las diferentes coyunturas críticas del trabajo de los periodistas y defensores de derechos humanos en los periodos de infección, surge un actor principal común: el gobierno federal.

La contundencia de la información y de los datos duros que demuestran los abusos en el uso *malware* Pegasus, adquirido por la Secretaría de la Defensa Nacional (SEDENA), la Procuraduría General de la República (PGR) y el Centro de Investigación y Seguridad Nacional (CISEN) es absoluta.

De acuerdo con el reportaje, "el Ejército Mexicano y la Fuerza Aérea Mexicana construyeron un Sistema de Inteligencia Regional para modernizar el Centro de Comando y Control, sus subcentros y módulos, y construir la Plataforma Pegasus." Tres contratos sobre la adquisición del sistema Pegasus por parte de la SEDENA fueron publicados el 16 de julio de 2012 por el portal Aristegui Noticias[43].

Sobre la PGR, el periódico *Reforma* publicó el 12 de septiembre de 2016 una nota en la que señalan que el gobierno mexicano pagó 15 millones de dólares por el sistema Pegasus, adquirido por el entonces fiscal Jesús Murillo Karam en 2014 y 2015. La afirmación coincide con una supuesta puja entre Hacking Team y NSO Group mencionada en uno de los correos filtrados por Hacking Team, fechado al 26 de agosto de 2014[44].

Está también documentado que el CISEN habló con representantes de NSO Group diciendo que ya habían probado otros programas que no necesitaban que la víctima le diera click al enlace para que se infectara.

---

42 Red en Defensa de los Derechos Digitales (R3D) (2017) Gobierno Espía. Vigilancia sistemática a periodistas y defensores de derechos humanos en México.
https://r3d.mx/2017/06/19/gobierno-espia/

43 Síntesis (2017) #GobiernoEspía ¿Qué es Pegasus y cómo funciona?
https://www.sintesis.mx/2017/06/19/gobiernoespia-que-es-pegasus-y-como-funciona/

44 Síntesis (2017) #GobiernoEspía ¿Qué es Pegasus y cómo funciona?
https://www.sintesis.mx/2017/06/19/gobiernoespia-que-es-pegasus-y-como-funciona/

Sistema Da Vinci / Galileo

El software Remote Control System (RCS), creado por la empresa italiana **Hacking Team**, es un software espía que se vende a organizaciones gubernamentales alrededor del mundo. **Da Vinci o Galileo** son los nombres comerciales de RCS. Es un software capaz de acceder a cualquier tipo de información contenida en una **computadora o teléfono celular**: contraseñas, mensajes y correos electrónicos, contactos, llamadas y audios de teléfono, micrófono y webcam, información de herramientas como Skype y otras plataformas de chat, posición geográfica en tiempo real, información almacenada en el disco duro, cada una de las teclas apretadas y clics del mouse, capturas de pantalla y sitios de Internet visitados, y más. En otras palabras, prácticamente todo lo que transcurre en un equipo personal[45].

Lo que distingue a RCS con el resto de formas de vigilancia tradicionales –como las escuchas telefónicas– es que no solo tiene acceso a conversaciones y comunicaciones, sino que puede capturar todo tipo de información, imágenes y datos que se encuentren en las computadoras o celulares afectados, **sin que sea necesario** que los mismos viajen por **Internet**[46].

Se instala de varias formas. Todos requieren un acto de "engaño" a la persona afectada. La primera forma en que puede instalarse es de manera física a través de una llave USB o usando un equipo especial llamado *Tactical Network Injector*, siempre y cuando las autoridades tengan acceso directo a la computadora. Por ejemplo, en un retén policial o cateos en aeropuertos. La segunda forma es mediante la emulación de una red de conexión inalámbrica a Internet (Wi-Fi) para ganar acceso a la computadora mediante un falso punto de conexión a Internet. También se puede vulnerar la clave de una red Wi-Fi existente para infiltrarse en ella. Para ello se requiere cercanía de quien quiere inocular el dispositivo de alguien más. La tercera forma es utilizando vías remotas o "no-físicas". El tipo más común es una falsa invitación por correo electrónico o adjuntos. También es común envío de mensajes de texto con falsas promociones que una vez se abren isntalan el *malware* en el equipo.[47]

45 Pérez de Acha, Gisela (2016) Informe: Hacking Team: Malware para la vigilancia en América Latina https://www.derechosdigitales.org/wp-content/uploads/malware-para-la-vigilancia.pdf
46 Pérez de Acha, Gisela (2016) Informe: Hacking Team: Malware para la vigilancia en América Latina https://www.derechosdigitales.org/wp-content/uploads/malware-para-la-vigilancia.pdf
47 Pérez de Acha, Gisela (2016) Informe: Hacking Team: Malware para la vigilancia en América Latina https://www.derechosdigitales.org/wp-content/uploads/malware-para-la-vigilancia.pdf

Un enlace así puede esconderse en cualquier tipo de tráfico no cifrado en Internet, por ejemplo streaming en videos de Youtube o Microsoft Live. Para esto se utiliza un equipo especial (llamado *Network Injector Appliance*) que se instala directamente a través de las empresas proveedoras de servicio y que, dependiendo de los patrones de tráfico, permite inocular a múltiples usuarios al mismo tiempo. Este método no requiere interceptación directa del usuario: basta con que se haga uso de Internet en el día a día. El uso de "exploits" es común en casi todos los métodos. Estos se aprovechan de los errores (bugs) y vulnerabilidades en sistemas computacionales con el propósito de introducir programas o funciones no consentidas por el usuario[48].

El Gobierno mexicano aparece como el cliente más importante de Hacking Team a nivel mundial, gastando un total de €5.808.875 por la compra de más de 15 licencias de espionaje. La empresa que funcionó como intermediaria en las negociaciones fue SYM Servicios Integrales[49].

México es el país con más clientes en la base de datos de la firma de hackers – 16 en total – los cuales han pagado en total cinco millones 808 mil 874 euros. Si además se suman las promesas de pago para 2015, la cifra asciende a seis millones 388 mil 784 euros, que equivalen a casi 111 millones de pesos[50].

Las negociaciones y compras de este software se hicieron en secreto hasta que el **5 de julio de 2015** se expusieron públicamente 400 GB e información de la empresa, incluyendo correos elctrónicos, facturas, documentación interna y parte del código de Hacking Team[51].

De acuerdo a lo filtrado hasta ahora, en el caso de Hacking Team aparecen clientes no autorizados por la Constitución: varias procuradurías estatales están haciendo vigilancia, en especial en zonas de violencia de alto impacto, donde hay menos controles que en el ámbito federal[52].

48 Pérez de Acha, Gisela (2016) Informe: Hacking Team: Malware para la vigilancia en América Latina https://www.derechosdigitales.org/wp-content/uploads/malware-para-la-vigilancia.pdf
49 Pérez de Acha, Gisela (2016) Informe: Hacking Team: Malware para la vigilancia en América Latina https://www.derechosdigitales.org/wp-content/uploads/malware-para-la-vigilancia.pdf
50 Angel, Arturo (2015) México, el principal cliente de una empresa que vende software para espiar. Animal Político. https://www.animalpolitico.com/2015/07/empresa-de-hackers-exhibida-por-venta-de-software-espia-a-paises-represores-y-mexico-resulta-su-principal-cliente/
51 Pérez de Acha, Gisela (2016) Informe: Hacking Team: Malware para la vigilancia en América Latina https://www.derechosdigitales.org/wp-content/uploads/malware-para-la-vigilancia.pdf
52 Rodríguez García, Arturo (2017) El caso Maloof y el software malicioso FinFisher. Revista Proceso. https://www.proceso.com.mx/491735/caso-maloof-software-malicioso-finfisher

El Centro de Investigación y Seguridad Nacional (CISEN), un organismo de inteligencia, realizó 2,074 órdenes judiciales para poder utilizar el software; hasta la fecha, no se sabe si su uso es justificado. Es el comprador número uno[53].

En México, un país que vive una seria crisis de derechos humanos, ocho de las diez autoridades que compraron RCS no están facultadas para ejercer actividades de vigilancia; pues además del CISEN varias dependencias realizaron su compra: la Procuraduría General de Justicia y los Cuerpos de Seguridad Auxiliar del Estado de México; la Secretaría de Seguridad Pública de Tamaulipas; la Secretaría de Planeación y Finanzas de Baja California; la Policía Federal; la Secretaría de Marina; Petróleos Mexicanos (PEMEX) y los estados de Jalisco, Querétaro, Puebla, Campeche y Yucatán[54].

Concretamente, en el estado de Puebla, el Gobierno utilizó las herramientas de Hacking Team para espiar a oponentes políticos, periodistas y estudiantes de la Universidad Iberamericana. Primero, al vigilar la campaña de un político de oposición llamado Ernesto Cordero y después a diversos periodistas a quienes enviaron correos engañosos para poder inocular sus aparatos[55].

En términos legales, este tipo de software no está regulado explícitamente en ningún país. En México y Colombia existen disposiciones amplias al respecto, pero con lenguaje vago e impreciso. La ausencia de regulación deja al arbitrio de las autoridades, muchas veces corruptos, el uso, aplicación y objetivos de RCS[56].

El 7 de julio, cuando la prensa cuestionó al Secretario de Gobernación Miguel Ángel Osorio Chong respecto a la compra del software de espionaje, el funcionario respondió que había sido

53 Romero, Mauricio (2016) Cisen: 2 mil 74 solicitudes para espiar con tecnología de Hacking Team". Revista Contralínea.
http://www.contralinea.com.mx/archivo-revista/index.php/2016/03/06/cisen-2-mil-74-solicitudes-para-espiar-con-tecnologia-de-hacking-team/

54 Angel, Arturo (2015) México, el principal cliente de una empresa que vende software para espiar. Animal Político.
https://www.animalpolitico.com/2015/07/empresa-de-hackers-exhibida-por-venta-de-software-espia-a-paises-represores-y-mexico-resulta-su-principal-cliente/

55 Aroche, Ernesto (2015) El gobierno de Puebla usó el software de Hacking Team para espionaje político. Animal Político.
http://www.animalpolitico.com/2015/07/el-gobierno-de-puebla-uso-el-software-de-hacking-team-para-espionaje-politico/

56 Pérez de Acha, Gisela (2016) Informe: Hacking Team: Malware para la vigilancia en América Latina
https://www.derechosdigitales.org/wp-content/uploads/malware-para-la-vigilancia.pdf

comprado por la administración pasada. Es decir, por otro partido en el periodo del presidente anterior. Por otro lado, los gobiernos de los estados de Jalisco, Yucatán, Durango y Campeche negaron toda relación con dicha empresa de espionaje. Ambas afirmaciones resultaron ser falsas. Llama la atención que la empresa siga operando. A pesar de la filtración y la publicación de los contratos entre Hacking Team y distintos organismos[57].

EVIDENCIAS Y OTRAS CONEXIONES:

Entre **2011 y 2012**, los dos últimos años del gobierno de Felipe Calderón, la Secretaría de la Defensa Nacional compró 350 millones de dólares en software de vigilancia para ser utilizado por el ejército mexicano, donde hubo una clara falta de transparencia en la compra y uso de este software[58].

2013: Privacy International, con una investigación, informó que la PGR había pagado hasta entonces 109 millones de pesos (mdp) por el software FinFisher y 93 mdp por un sistema de seguimiento por satélite llamado Hunter Punta Tracking / Locsys. Ambas compras se realizaron a la empresa Obses[59].

Durante las semanas de las denuncias y el informe de Toronto, dos altos ejecutivos de Gamma International visitaron diferentes dependencias mexicanas. Según documentó Wikileaks, Carlos Gandini estuvo en febrero de 2013 en México y el técnico Martin Muench (quien desarrolló FinFisher) llegó el 23 de abril y se fue tres días después.

Con las rutas de investigación bloqueadas, Robles Maloof encontró otra relación a partir de un pasaje del libro México en llamas, de Anabel Hernández, donde se informa que Obses es una empresa de Gustavo Cárdenas Moreno, familiar de Luis Cárdenas Palomino, uno de los colaboradores más cercanos a García Luna (secretario de seguridad). A decir de la autora, ambos

57 Pérez de Acha, Gisela (2016) Informe: Hacking Team: Malware para la vigilancia en América Latina https://www.derechosdigitales.org/wp-content/uploads/malware-para-la-vigilancia.pdf
58 SonTusDatos (2014) El caso FinFisher. https://www.giswatch.org/hu/node/4955
59 SonTusDatos (2014) El caso FinFisher. https://www.giswatch.org/hu/node/4955

se distanciaron por un pleito relacionado con el reparto de las comisiones de los contratos con Obses.

Cárdenas Palomino es cuñado del actual consejero jurídico de la Presidencia de la República, Humberto Castillejos Cervantes.

Un comparativo realizado por Robles Maloof permitió determinar que FinFisher se vendió al gobierno mexicano en montos cuatro veces superiores a lo que se cotizan en el extranjero. En tanto, organizaciones internacionales que han dado seguimiento al caso señalaron que, conforme a las leyes de la Unión Europea, a las que se atiene Gamma International, sus ventas deben ser directas, sin intermediarios y sólo a gobiernos. Obses operó entonces al margen de acuerdos internacionales.

Aún peor. Cuando el 4 de septiembre de 2014, el hacker PhineasFisher anunció que había hackeado a Gamma International, entre sus clientes apareció Cobham Defence Electronics, contratista de servicios e insumos de seguridad en México, de manera que no sólo vendían a gobiernos[60].

Además de la utilización de *malware* es importante señalar las cifras de peticiones de investigación que el gobierno hizo a redes sociales recientemente: En 2014, pidió a Facebook información sobre 679 usuarios; en el primer semestre del mismo año había realizado pedimentos sobre 111 cuentas a Google, 460 a Microsoft para 705 usuarios, 89 peticiones a Yahoo y 5 a Twitter[61].

También es importante no perder de vista el caso de la reciente reforma en materia de telecomunicaciones. Una nueva preocupación surgió entre los interesados en el tema, tanto en la clase política como en la sociedad civil, por la redacción del artículo 189 de la Ley Federal de Telecomunicaciones y Radiodifusión, porque su ambigüedad parece autorizar a procuradurías estatales a tramitar, sin orden judicial, geolocalizaciones, escuchas e intervención de comunicaciones[62].

60 Rodríguez García, Arturo (2017) El caso Maloof y el software malicioso FinFisher. Revista Proceso. https://www.proceso.com.mx/491735/caso-maloof-software-malicioso-finfisher
61 Rodríguez García, Arturo (2017) El caso Maloof y el software malicioso FinFisher. Revista Proceso. https://www.proceso.com.mx/491735/caso-maloof-software-malicioso-finfisher
62 Rodríguez García, Arturo (2017) El caso Maloof y el software malicioso FinFisher. Revista Proceso. https://www.proceso.com.mx/491735/caso-maloof-software-malicioso-finfisher

Tabla 1. Autoridades con evidencia de adquisición de equipo sofisticado de vigilancia en México

	NSO Group (Israel): Pegasus	Hacking Team (Italia): Remote Control System (DaVinci/Galileo)
Autoridades Federales	• ***Sí:*** Procuraduría General de la República (fuente) • ***Sí:*** Secretaría de la Defensa Nacional (SEDENA) (fuente) • ***Altamente probable:*** Centro de Investigación y Seguridad Nacional (CISEN) (fuente)	• ***Altamente probable:*** Procuraduría General de la República (fuente) • ***Altamente probable:*** Secretaría de la Defensa Nacional (SEDENA) (fuente) • ***Sí:*** Centro de Investigación y Seguridad Nacional (CISEN) (fuente) • ***Sí:*** Policía Federal (fuente) • ***Sí:*** Petróleos Mexicanos (fuente)
Autoridades estatales	• Ninguna documentada hasta el momento	• Gobierno estatal de: • ***Sí:*** Baja California (fuente) • ***Sí:*** Campeche (fuente) • ***Altamente probable:*** Chihuahua (fuente) • ***Sí:*** Durango (fuente) • ***Sí:*** Guerrero (fuente) • ***Sí***: Jalisco (fuente) • ***Altamente probable:*** Nayarit • (fuente) • ***Sí:*** Puebla (fuente) • ***Sí:*** Querétaro (fuente) • ***Altamente probable:*** Sonora (fuente) • ***Sí***: Tamaulipas (fuente) • ***Sí:*** Yucatán (fuente) • ***Sí:*** Procuraduría General del Estado de México (fuente)

* REFERENCIAS (por orden de aparición)

-R3D (2019): "No soy criminal ni terrorista, pero fui espiada": Griselda Triana, viuda de Javier Valdez, fue atacada con Pegasus. https://r3d.mx/2019/03/20/no-soy-criminal-ni-terrorista-pero-fui-espiada-griselda-triana-viuda-de-javier-valdez-fue-atacada-con-pegasus/

-Bauman, Zygmunt y David Lyon (2013) Vigilancia líquida. Paidós

-Sparrow, Elijah (2014) Vigilancia digital
https://giswatch.org/es/thematic-report/communications-surveillance/vigilancia-digital

-Rivero, Marcelo (2016) ¿Qué son los malwares?
https://www.infospyware.com/articulos/que-son-los-malwares/

-Pérez de Acha, Gisela (2017) ¿Quién está utilizando malware en México?
https://www.derechosdigitales.org/10874/quien-esta-utilizando-malware-en-mexico/

-Wikipedia: Ingeniería social (seguridad informática)
https://es.wikipedia.org/wiki/Ingenier%C3%ADa_social_(seguridad_inform%C3%A1tica)

-"Ingeniería social" (s/f) Departamento de Seguridad Informática de la Universidad Nacional de Luján.
http://www.seguridadinformatica.unlu.edu.ar/?q=taxonomy/term/11

-Pérez de Acha, Gisela (2016) Informe: Hacking Team: Malware para la vigilancia en América Latina
https://www.derechosdigitales.org/wp-content/uploads/malware-para-la-vigilancia.pdf

-Red en Defensa de los Derechos Digitales (R3D) (2016) El estado de la Vigilancia: Fuera de control.
https://r3d.mx/wp-content/uploads/R3D-edovigilancia2016.pdf

-SonTusDatos (2014) El caso FinFisher.
https://www.giswatch.org/hu/node/4955

-Ángel, Arturo (2015) México, el principal cliente de una empresa que vende software para espiar. Animal Político.
https://www.animalpolitico.com/2015/07/empresa-de-hackers-exhibida-por-venta-de-software-espia-a-paises-represores-y-mexico-resulta-su-principal-cliente/

-Rodríguez García, Arturo (2017) El caso Maloof y el software malicioso FinFisher. Revista Proceso. https://www.proceso.com.mx/491735/caso-maloof-software-malicioso-finfisher

-Red en Defensa de los Derechos Digitales (R3D) (2017) Gobierno Espía. Vigilancia sistemática a periodistas y defensores de derechos humanos en México. https://r3d.mx/2017/06/19/gobierno-espia/

-Red en Defensa de los Derechos Digitales (R3D) (2016) Vigilancia Estatal de las Comunicaciones y Protección de los Derechos Fundamentales en México. https://necessaryandproportionate.org/es/country-reports/mexico

-Flores, Pepe (2015) FinFisher en México: Sonríe, te siguen espiando. https://www.digitalrightslac.net/es/finfisher-en-mexico-sonrie-te-siguen-espiando/

-Red en Defensa de los Derechos Digitales (R3D) (2017) Destapa la vigilancia: promotores del impuesto al refresco, espiados con malware gubernamental. https://r3d.mx/2017/02/11/destapa-la-vigilancia-promotores-del-impuesto-al-refresco-espiados-con-malware-gubernamental/

-Ahmed, Azam y Nicole Perlroth (2017) 'Somos los nuevos enemigos del Estado': el espionaje a activistas y periodistas en México. New York Times. https://www.nytimes.com/es/2017/06/19/mexico-pegasus-nso-group-espionaje/

-Red en Defensa de los Derechos Digitales (2017) Promotores del impuesto al refresco, espiados con malware gubernamental. Lado B. https://ladobe.com.mx/2017/02/destapa-la-vigilancia-promotores-del-impuesto-al-refresco-espiados-malware-gubernamental/

-Síntesis (2017) #GobiernoEspía ¿Qué es Pegasus y cómo funciona? https://www.sintesis.mx/2017/06/19/gobiernoespia-que-es-pegasus-y-como-funciona/

-Romero, Mauricio (2016) Cisen: 2 mil 74 solicitudes para espiar con tecnología de Hacking Team". Revista Contralínea. http://www.contralinea.com.mx/archivo-revista/index.php/2016/03/06/cisen-2-mil-74-solicitudes-para-espiar-con-tecnologia-de-hacking-team/

-Aroche, Ernesto (2015) El gobierno de Puebla usó el software de Hacking Team para espionaje político. Animal Político. http://www.animalpolitico.com/2015/07/el-gobierno-de-puebla-uso-el-software-de-hacking-team-para-espionaje-politico/